UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN

EPIC SYSTEMS CORPORATION, a Wisconsin Corporation, Plaintiff, v. TATA CONSULTANCY SERVICES LIMITED, an Indian Corporation; and TATA AMERICA INTERNATIONAL CORPORATION (dba TCS AMERICA), a New York Corporation, Defendants.	Case No. 14-CV-748 **REDACTED**

OPPOSITION TO DEFENDANTS' MOTION TO DISMISS PLAINTIFF'S AMENDED COMPLAINT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

OTHER AUTHORITIES

INTRODUCTION AND SUMMARY

The motion to dismiss should be denied. Epic has alleged ample evidence of TCS's wrongdoing in the Amended Complaint and the law supports all of the causes of action that have been asserted.

TCS claims that Epic has not provided enough facts for most of the causes of action. Further, TCS argues that the whole case deserves dismissal because the facts that have been alleged are "implausible." TCS attacks its key employee, Philippe Guionnet, who revealed that TCS was stealing information from Epic to advance TCS's own competitive product known as Med Mantra. TCS says "Mr. Guionnet may not be telling the truth about Med Mantra." Mot. at 26. TCS denigrates Mr. Guionnet as "a so-called 'informant,'" who made up a "story" about TCS stealing Epic's information for the benefit its Med Mantra product, based on what TCS calls mere "suspicions" "speculation," and "speculative assertions." *Id*. at 3, 25, 26, 32. TCS insinuates there are no "facts to demonstrate that even a single piece of the information allegedly accessed by TCS has been, or could be, used in connection with Med Mantra." *Id*. at 2.

Not surprisingly, TCS would prefer to have this case tossed out of the courthouse rather than confront the truth of its misconduct, both in the United States and in India. The evidence of TCS's misconduct is all over the Amended Complaint and is beginning to come forth in early discovery returns as well.

Neither of the two principal grounds on which TCS bases it dismissal motion withstand scrutiny, as we explain more fully below. We start with a factual background section, in which we set the record straight about the allegations of the Amended Complaint, which were only selectively portrayed in the dismissal motion. Then, in a two-part argument section, we explain why the dismissal motion should be denied.

In Part I, we address the "implausibility" argument. Contrary to what TCS says, the facts alleged in this lawsuit are demonstrably plausible. The many critical facts alleged here are more than sufficient in our "notice" pleading system, which is designed to put the defendant on enough notice to mount a defense. The Amended Complaint describes how TCS personnel masqueraded as Epic's employees, misrepresented their true identities as consultants, and thereby exceeded their authorized scope of access to Epic's UserWeb. Those TCS personnel improperly took confidential information out of Epic's UserWeb, downloaded thousands of documents, sent the information to India, and then used the information to help TCS with its own competitive product called Med Mantra. Most of the allegations are based on evidence uncovered by Epic during in its own investigation that began after Mr. Guionnet disclosed TCS's misconduct. Other allegations are based on statements by Mr. Guionnet that will be subject to further confirmation during the discovery process.

To take a concrete example, an email chain in the possession of TCS and its lawyers before the Amended Complaint, but not produced until after the Amended Complaint was filed, demonstrates that Mr. Guionnet's statements are not just plausible, but are reliable and true. Indeed, it is hard to understand how a TCS lawyer could write about "implausibility" with the pen in his right hand, while holding the damning email chain in his left hand. The email chain is not necessary for the Court to deny the dismissal motion, but it certainly confirms the plausibility of the grounds on which this lawsuit is brought.

In Part II of the argument, we demonstrate that Epic's causes of action are well supported not just by the facts, but also the law. For example, TCS claims that Epic cannot pursue claims under the Computer Fraud and Abuse Act ("CFAA") because it has not alleged that TCS's access to the UserWeb was either unauthorized or exceeded authorization. The Seventh Circuit, however, has held that TCS's failure to act in accordance with its contractual obligations, which defined the parameters of its UserWeb authorization, is a sufficient basis on which to hold TCS liable under the CFAA. Further, although TCS argues that Epic has not stated a viable claim for breach of contract, it ignores the allegations in the Amended Complaint setting forth the details of TCS's contractual obligations, and the numerous ways in which TCS failed to meet those obligations. Instead, TCS tries to hold Epic to a pleading standard above and beyond that articulated by any federal court. All of TCS's arguments suffer from similar infirmities.

FACTUAL BACKGROUND

I. Epic Develops its Software Applications Through Decades of Hard Work.

Epic is a Wisconsin-based healthcare company that makes software for mid-size and large medical groups, hospitals, and integrated healthcare organizations. ECF No. 38 ("Am. Compl.") ¶ 2. Epic's software manages the collection and storage of patient data and care process data into a common database, including records of patient admissions and discharges, pharmacy, specialty care, billing, insurance benefits, and referral information. *Id.*

The know-how and development of Epic's software is the result of careful, hard work by Epic's employees at a tremendous monetary cost and expenditure of man-hours over a period of decades. *Id.* Epic's intellectual property, confidential information, documents, and trade secrets are important to Epic and, thus, the company takes reasonable means to protect those assets. *Id.* ¶ 4. Epic shares its confidential information and trade secrets with its employees and certain customers subject to confidentiality obligations, which are designed to protect Epic's computer network, software, documents, confidential information, and trade secrets. *Id.*

II. Epic Limits Access to its Confidential Information on the UserWeb.

At the heart of this dispute is Epic's UserWeb system, which is a protected electronic workspace through which Epic provides training and other user materials, such as program manuals, to assist its customers with their implementation and maintenance of Epic products. Am. Compl. ¶ 17. Access to the Epic UserWeb is limited to those who require Epic information in order to facilitate installation, maintenance, or support of Epic software in use by a particular customer of Epic. *Id.* ¶ 19.

The UserWeb registration form requires each registrant to provide his or her employer information, including whether the registrant is a direct "employee of an Epic customer," or a once-removed "consultant" for an Epic customer. Am. Compl. ¶ 20. Direct employees of Epic customers are granted access to the Epic UserWeb without additional restrictions. This is because the customer has already contractually promised not to wrongfully use or disclose Epic documents or information, usually in a detailed written agreement governing the entire relationship between Epic and the customer. *Id.* Secondary consultants who have been hired by customers, on the other hand, are required to complete an additional UserWeb Access Agreement before their account can be considered for approval and authorization for access granted by Epic. *Id.* ¶ 21. The additional consultant agreement is designed to provide another layer of protection for Epic before the consultants are authorized to access Epic's UserWeb. *Id.* This is because some of the consultants work for companies (like TCS) that compete with Epic.

If identified as a consultant, a person is not eligible to obtain access to the UserWeb until his or her consulting firm has entered a Consultant Access Agreement with Epic for the applicable customer. Am. Compl. ¶ 22. The specifics of the Consultant Access Agreement are designed to limit the consultant's use of information and protect Epic from any improper use or disclosure of its software, documents, trade secrets, confidential information, intellectual property, or the other valuable information on the Epic UserWeb. *Id.* Importantly, even if a secondary consultant is granted access to the UserWeb, that access is more limited than the access granted to Epic's direct customers. *Id.* ¶ 23. Epic purposefully circumscribes a consultant's access to a limited area that is necessary for the consultant to support the customer. *Id.* In other words, just having permission to enter into the UserWeb does not answer the question of how much access is authorized. The extent of the authorization is defined by the identity of the user. A direct customer user has greater access as a result of a more expansive authorization. A secondary consultant user has more limited access as a result of his or her more restrictive authorization.

III. <u>Epic Enters into a Licensing Agreement with Kaiser.</u>

On February 4, 2003, Epic entered into a written agreement with Kaiser (the "Kaiser Agreement") under which Epic agreed to license certain computer software to Kaiser to support patient care delivery activities at all of Kaiser's venues. Am. Compl. ¶ 16. The Kaiser Agreement contains provisions protecting Epic's confidential information by allowing dissemination of information only to persons with a need to know, and limiting the uses to those needed to fulfill the purpose of the Kaiser Agreement. *Id.* ¶ 17. Pursuant to the Kaiser Agreement, Epic provided Kaiser access to Epic's UserWeb. *Id.*

IV. <u>Epic Enters into a Consultant Agreement with TCS.</u>

In August 2005, Epic became aware that Kaiser had hired TCS consultants to support its complex computer networks and software systems, including Epic software, when several individuals claiming to be Kaiser employees registered with Epic to receive certain software training classes. Am. Compl. ¶ 26. However, those individuals were employed by TCS, not

Kaiser. *Id*. Epic removed the TCS employees from the Epic training course and informed them that TCS personnel could not be trained on Epic software until Epic received an executed non-disclosure agreement from TCS. *Id.*

Epic and TCS America then entered a Standard Consultant Agreement (the "TCS America Agreement") whereby Epic agreed to allow certain TCS employees access to Epic training programs for the limited purposes of providing consulting services to Epic's customers related to the implementation of "Epic Program Property." *Id.* ¶ 27. The TCS America Agreement defines Epic Program Property as the "computer program object and source code and the Documentation for all of Epic's computer programs." *Id.* ¶ 28. The TCS America Agreement imposes on TCS the following obligations:

- to "limit access to the Program Property to those [TCS employees] who must have access to the Program Property in order to implement the Program Property on Epic's or its customer's behalf" (i.e., Kaiser). Am. Compl. ¶ 29(a);
- not to "use the Program Property . . . for any other purpose other than in-house training of [TCS] employees to assist Epic customers in the implementation of the Program Property licensed by that Epic customer." *Id.* ¶ 29(b);
- to "use Confidential Information only for the purpose of implementing the Program Property on an Epic customer's behalf." *Id.* ¶ 29(d); and
- not permit any employee who has had access to the Program Property to participate in any "development, enhancement or design of, or to consult, directly or indirectly, with any person concerning any development, enhancement or design of, any software that competes with or is being developed to compete with Epic Program Property . . . ." *Id.* ¶ 29(f).

TCS has continued to provide consulting services to Kaiser related to the implementation and maintenance of Epic Program Property since 2005. *Id*. ¶ 31. Although Epic terminated the TCS America Agreement shortly after filing this lawsuit, the confidentiality and use restrictions articulated in the agreement remain in effect "for the maximum duration and scope allowed by law." *Id.* ¶ 30.

V. TCS Engages in Unauthorized Access, Fraud, and Theft of Epic's Information.

A. Mr. Guionnet Informs Epic of TCS's misconduct.

In late May 2014, Epic first learned from TCS employee Philippe Guionnet that TCS personnel had been, fraudulently and without authorization, accessing Epic's UserWeb computer network, and that the information obtained through the unauthorized access into UserWeb was being used by TCS to benefit its competing Med Mantra software. Am. Compl. ¶ 33.

Mr. Guionnet was in a position to know this information, as he was responsible for managing all aspects of TCS's contract with Kaiser to provide consulting services until May 2014, and he reported directly to TCS executive management. *Id.* ¶¶ 33, 56. Mr. Guionnet's duties included, among other things, making decisions on the Kaiser account, holding and attending regular staff meetings and client meetings, travelling with the client to India and attending technical, sales, and marketing activities specific to the Kaiser account, and submitting financial forecasts on a weekly basis. *Id.* ¶ 56. Further, his team "had a substantial dotted line to a Global Group also called Care Delivery (typically including Hospitals i.e. MedMantra, lab, ambulatory, etc.)," and "Operation & Delivery for Kaiser (including Epic support from India) ultimately reported to the same person in charge of Care Delivery." *Id.* ¶ 59.

As part of his job responsibilities, Mr. Guionnet was "exposed to various MedMantra products and services multiple times" (*id.* ¶ 60), and he participated in marketing MedMantra products to Kaiser (*id.* ¶ 63). In particular, Mr. Guionnet "was asked to identify if some MedMantra modules would fit at Kaiser," "specifically reviewed some MedMantra functionalities and modules as an option to be implemented at Kaiser," and "specifically reviewed at length some MedMantra functionalities and modules in Laboratory as an option to be implemented at Kaiser." *Id.* Mr. Guionnet also confirmed that he "saw, and/or suspected, and/or was aware of several comparisons between MedMantra and Epic softwares, including by the MedMantra team." *Id.* ¶ 64. With respect to development of MedMantra, Mr. Guionnet stated that "[r]egulatory and Hospital requirements have been notoriously a source of obstacle, frustration and costs to MedMantra/TCS to enter the US market as a whole, they have been allegedly a 'source of interest,'" and that some of the confidential information that TCS took from Epic contains information regarding "how they are handled at Kaiser in the Epic system." *Id.* ¶ 62.

According to Mr. Guionnet, TCS's unauthorized access to Epic information began as early as 2012, and TCS leaders in the United States and India were aware of and complicit in TCS's scheme to unlawfully access Epic's UserWeb to misuse confidential Epic information and valuable intellectual property for the benefit of TCS. *Id.* ¶ 34. Mr. Guionnet further described that an access credential for the UserWeb had been used by TCS personnel in India to access Epic's UserWeb without authorization and improperly download information including Program Property and Confidential Information within the meaning of the TCS America Agreement. *Id.* ¶ 35. The purpose of the misconduct was to use information and documents related to Epic's leading software to benefit TCS's creation of and improvements to TCS's competing Med Mantra product. *Id.*

B. Epic Confirms TCS's Unauthorized Downloading of Thousands of Epic Files.

After learning of the unauthorized and illegal downloading of Epic information by TCS personnel, and the apparent purpose of the misconduct, Epic investigated its protected UserWeb and discovered that an account associated with Ramesh Gajaram, a TCS employee who worked as a consultant for Kaiser in Portland, Oregon, and who worked on projects related to Epic's provision of software and services to Kaiser, had downloaded from Epic's UserWeb at least

6,477 documents accounting for ***1,687 unique files***. Am. Compl. ¶ 36. These documents included Program Property and Confidential Information within the meaning of the TCS America Agreement. *Id*.

Specifically, the documents downloaded by TCS personnel included, among other things, confidential, proprietary, and trade secret documents detailing over twenty years of development of Epic's proprietary software and database systems, including: programming rules and processes developed to produce optimal functionality of Epic's software; documents that decode the operation of its source code that would otherwise be unusable to those outside of Epic; and information regarding Epic's system capabilities and functions, including procedures for transferring data between customer environments, rules related to information collection, methods for limiting access to patient records, and processes for converting customer data, all of which reveal decades of Epic's work with its customers to determine the functionality desirable or required for Epic to provide successful products to those customers. *Id*. ¶ 39.

Many of the downloaded Epic documents were not required for Mr. Gajaram to be able to perform his own job functions in support of Kaiser. *Id.* ¶ 40. For example, the downloaded Epic documents include a guide containing confidential and/or trade secret information that provides a blueprint for understanding Epic's source code or competing with Epic's infrastructure. *Id.*

Mr. Gajaram's access credentials were used to access the Epic UserWeb from an IP address in India during the time when Mr. Gajaram worked in Portland, Oregon. *Id*. ¶ 37. Mr. Gajaram's access credentials were also utilized from other IP addresses around the United States, outside of Oregon, during that same time period. *Id.* Mr. Gajaram's credentials were used to download documents from IP addresses in India registered to TCS. This means that someone else within TCS, but outside the Kaiser network, used Mr. Gajaram's login credentials as if they were Mr. Gajaram. *Id.* Epic therefore was able to confirm much of Mr. Guionnet's information regarding TCS's misconduct. *Id.*

In fact, when confronted by Kaiser regarding this downloading of Epic data, Mr. Gajaram admitted that he had downloaded the Epic documents, and that he had provided his Epic access credentials to at least two other TCS employees, Aswin Kumar Anandhan and Sankari Gunasekaram, in violation of the UserWeb Access Agreement. *Id.* ¶¶ 47, 38. Neither Mr. Anandhan nor Mr. Gunasekaram were authorized to use those credentials and they had not received permission or authorization to take Epic information from Epic's UserWeb. *Id.* ¶ 38. Mr. Gajaram admitted that these other TCS personnel did not need access to the Epic UserWeb to be able to perform job functions in support of Kaiser. *Id.* ¶ 47.

C. Epic Learns that Mr. Gajaram Fraudulently Obtained his UserWeb Credentials.

In addition to the enormous number of downloads accomplished through the misuse of Mr. Gajaram's UserWeb log-in credentials, it was discovered that Mr. Gajaram had obtained his credentials in a fraudulent manner. Am. Compl. ¶ 41. When Mr. Gajaram registered for the UserWeb, he misrepresented that he was a "customer employee" instead of a "consultant," even though Epic requires consultants to specifically identify themselves as such. *Id.* He also used a "kp.org" email address, which Kaiser provides to its consultants for use while consulting for Kaiser, to further mislead Epic into believing that Mr. Gajaram was an employee of Kaiser when he was in fact an employee of TCS. *Id.*

Mr. Gajaram appears to have intentionally misrepresented himself as a Kaiser employee for the purpose of avoiding the restrictions of the UserWeb Access Agreement that apply to consultants and gaining customer-level access authorization to the UserWeb. *Id.* ¶ 42. By gaining customer-level access, rather than consultant access, Mr. Gajaram exceeded the access granted by Epic to TCS personnel for the limited purposes of implementing, integrating, or testing Epic's software at Kaiser. *Id.* Upon discovery of the fraudulent access to, and excessive downloading from, the Epic UserWeb by Mr. Gajaram, Epic suspended Mr. Gajaram's User ID so that no further access or downloading could occur. *Id.* ¶ 43.

Shortly thereafter, Mr. Gajaram sought via email to have his access to the UserWeb reactivated so that he could, once again, gain access to the UserWeb. *Id.* ¶ 44. He sent two emails on June 24 and June 30, 2014, seeking reactivation of his account. *Id.* The first email, on June 24, included a signature line indicating that his title was "QA Lead, Kaiser Permanente." *Id.* The second email, on June 30, included a different signature line indicating that Mr. Gajaram was actually an "Onshore Test Lead" for TATA Consultancy Services, as well a "QA Lead" title for Kaiser. *Id.* Mr. Gajaram appears to have understood that the access he sought exceeded access that would be granted to a consultant. He also appears to have tried multiple times to regain his access knowingly using different postures, once masquerading as a Kaiser employee and then again in his true identity as a TCS consultant. *Id.*

There appears to be no legitimate reason for Mr. Gajaram, and those with whom he was conspiring at TCS, to download more than six thousand files from Epic, or to download some of the specific pieces of confidential data he targeted on the Epic system. *Id.* ¶ 45. Mr. Gajaram would not have needed much of the information that he downloaded to perform his limited job function supporting Kaiser, to say nothing of Mr. Anandhan or Mr. Gunasekaram. *Id.* TCS employees downloaded certain documents that were not available to consultants for Kaiser. *Id.* For example, Mr. Gajaram only gained access to confidential and/or trade secret documents such as the Community Connect Install Summary, ADT End-User Proficiency Question Bank, ED

Registrar Checklist, and the Physician's Guide to EpicCare Ambulatory zip file (among many others), by fraudulently representing himself as a Kaiser employee. *Id*.

D. Epic Has Been Harmed by TCS's Wrongful Acts.

To date, Epic has incurred far more than $5,000 in costs and losses related to investigating Defendants' unauthorized access to Epic's UserWeb. *Id.* ¶ 50. Epic will continue to incur costs, losses, and damages as it seeks to uncover how much of its intellectual property, trade secrets, confidential information, internal documents, and other Epic information and data was taken by TCS personnel. *Id.*

Unless restrained by this Court, TCS's unauthorized access to Epic's intellectual property, trade secrets, confidential information, internal documents, and other information and data, and subsequent theft of Epic's intellectual property, trade secrets, confidential information, internal documents, and other information and data by downloading from the UserWeb, will allow TCS to shortcut years of hard work and investment expended by Epic in developing Epic's industry-leading medical software products. *Id.* ¶ 52.

ARGUMENT

I. EPIC SATISFIES THE PLAUSIBILTY STANDARD.

In deciding a motion to dismiss, the Court ultimately must determine whether the defendant is on sufficient notice of the factual and legal bases for the claims against it, so that the defendant might mount an appropriate defense. That is the theory behind our federal system of notice pleading, which remains unchanged by the "implausibility" gloss applied by *Bell Atl. Corp. v. Twombly*, 550 U.S. 544 (2007) and *Ashcroft v. Iqbal*, 556 U.S. 662 (2009).

The Seventh Circuit has summarized *Twombly* and *Iqbal* as follows: "First, a plaintiff must provide notice to defendants of her claims. Second, courts must accept a plaintiff's factual allegations as true, but some factual allegations will be so sketchy or implausible that they fail to provide sufficient notice to defendants of the plaintiff's claim. Third, in considering the plaintiff's factual allegations, courts should not accept as adequate abstract recitations of the elements of a cause of action or conclusory legal statements." *Brooks v. Ross*, 578 F.3d 574, 581 (7th Cir. 2009).

Although *Twombly* and *Iqbal* may have "created a plausibility standard that requires courts to apply a somewhat heightened standard of scrutiny to a complaint's factual allegations," they "did not alter the landscape in terms of [the notice] pleading law." *Hedeen Intern., LLC v. OzWest, Inc.*, No. 14-304, 2014 WL 5682507, at *1 (E.D. Wis. Nov. 4, 2014); *Bissessur v. Ind. Univ. Bd. of Trustees*, 581 F.3d 599, 603 (7th Cir. 2009) ("Our system operates on a notice pleading standard; *Twombly* and its progeny do not change this fact.").

A. <u>The Amended Complaint's Allegations Are Plausible</u>.

Rather than deal with the factual allegations head on, TCS tries to avoid them by attacking Mr. Guionnet, arguing that his revelations are merely a "story" that is based on nothing more than implausible "speculation" and "suspicion." *E.g.*, Mot. at 3, 25, 26, 32. But TCS provides no real basis on which to discredit Mr. Guionnet's first-hand knowledge other than saying "Mr. Guionnet may not be telling the truth about Med Mantra." Mot. at 26. A credibility attack is not a sufficient basis here on which to dismiss the complaint.

In *Makor Issues & Rights, Ltd. v. Tellabs Inc.*, 513 F.3d 702 (7th Cir. 2008), the Seventh Circuit analyzed the plausibility of allegations based on information provided by confidential informants. In holding that the allegations were sufficient to meet the *heightened* pleading requirements of the Private Securities Litigation Reform Act, the court found it particularly significant that the informants were "persons who from the description of their jobs were in a position to know at first hand the facts to which they are prepared to testify." *Id.* at 712. Further, "[t]he information that the confidential informants are reported to have obtained is set forth in convincing detail, with some of the information, moreover, corroborated by multiple sources." For this reason, the court "reverse[d] the judgment of the district court dismissing the suit." *Id.*

Here, similarly, Mr. Guionnet was in a position to have first-hand knowledge about TCS's unauthorized access to Epic's information, as well as the use of that information to benefit TCS's Med Mantra product. In particular, Mr. Guionnet was responsible for managing all aspects of TCS's contract with Kaiser, through which Mr. Gajaram and others acquired unauthorized access to the UserWeb. Am. Compl., ¶ 56. In that position, Mr. Guionnet had frequent communications with TCS executive management (*id.*) and traveled with Kaiser to India (*id*., ¶ 56). Also, Mr. Guionnet was "exposed to various MedMantra products and services multiple times," (*id*., ¶ 60), including marketing MedMantra products to Kaiser (*id*., ¶ 63) and "specifically review[ing] some MedMantra functionalities and modules as an option to be implemented as Kaiser." (*Id.*, ¶ 63). These facts and others, as alleged in the Amended Complaint, provide a sufficient basis on which to conclude that Mr. Guionnet was "in a position to know at first hand the facts to which [he is] prepared to testify." *Tellabs*, 513 F.3d at 712.

Mr. Guionnet's information has also been corroborated by independent investigation, including Epic's own investigation into the thousands of documents downloaded by TCS personnel in the United States and India, as well as Mr. Gajaram's admissions in the course of Kasier's independent investigation. Am. Compl. ¶¶ 36-37, 46-47. This independent corroboration further supports the veracity of Mr. Guionnet's statements, which achieve the requisite plausibility to meet the basic pleading standard under Rule 8(a).

B. Plausibility Is Confirmed by Evidence Produced Prior to the Dismissal Motion.

We agree with TCS that the Court should "draw on its judicial experience and common sense" in making the determination about whether TCS is on sufficient notice of the claims against it. *See* Mot. at 13 (quoting *Thulin v. Shopko Stores Operating Co., LLC*, 771 F.3d 994, 997 (7th Cir. 2014) and *Ashcroft v. Iqbal*, 556 U.S. 662, 679 (2009)). In this context, we believe the Court should be aware that TCS produced evidence prior to the filing of its dismissal motion, but after the Amended Complaint was filed, that confirms the plausibility of Epic's allegations in this lawsuit.

Here, the Amended Complaint was filed on January 26, 2015. ECF No. 38. Four days later, on January 30, TCS made a small initial document production, which included the relevant email chain. Spelman Decl. ¶ 2.[1] Ten days later, on February 9, 2015, TCS filed its dismissal motion. ECF No. 43. As a result, while the email chain was known to TCS before the Amended Complaint was filed, TCS waited to produce it until after Epic filed the Amended Complaint, deriving Epic of the opportunity to quote it in the amendment. In any event, no matter why or when the email chain was produced, it shines a bright and focused light on the "who, what, when, where, and how of the alleged fraud" and other misconduct TCS claims it does not understand. *See* Mot. at 36.

In a dozen emails sent in the second half of March 2014, it is clear that [redacted]

[1] TCS made this production as a result of Epic's Motion for Expedited Discovery, which Judge Crocker granted in part on December 8, 2014, and Epic's subsequent Motion to Compel Compliance with Court Order, which Judge Crocker granted in part on January 23, 2015. ECF Nos. 21, 37.

[redacted] What follows is a brief summary of the email chain.

Starting chronologically, on March 19, 2014, [redacted]

[redacted]

[redacted] Publicly, Mr. Yallapragada refers to himself as “Dr.

[2] All exhibits cited herein are attached to the concurrently-filed Declaration of Kate T. Spelman.

Naresh Yallapragada" and is part of the "product management group" at TCS. Ex. 2. His activities include "market research," "market segmentation and analysis," "analysis on product certifications," "product road map," "product marketing," and "product demonstration to potential clients." *Id.* [redacted]

Later in the email chain, on March 24, 2014, [redacted]

[redacted]

[redacted]

[redacted]

[redacted] Indeed, by the end of the email chain, it is crystal clear that Mr. Guionnet's statements are not only plausible, but true, when he said [redacted]

The email chain verifies Mr. Guionnet's account and demonstrates that he is not a speculative story teller. But, in any event, if there is a credibility fight going on here between Mr. Guionnet and TCS, that is no basis for granting dismissal. Rather, it is a basis to deny the dismissal motion. The bottom line is that the allegations in the Amended Complaint are plausible, both taken at face value and as confirmed by the evidence provided in discovery to date.[3]

We will now work our way through the Amended Complaint in Part II of the argument section below.

II. ALL OF THE CAUSES OF ACTION PROPERLY STATE CLAIMS ON WHICH RELIEF CAN AND SHOULD BE GRANTED.

A. Epic States a Claim under the Computer Fraud and Abuse Act.

The Computer Fraud and Abuse Act ("CFAA") creates a civil cause of action for "[a]ny person who suffers damage or loss by reason of a violation of this section . . . to obtain compensatory damages and injunctive relief or other equitable relief" if the conduct complained of involves one of the factors set forth in subsection (c)(4)(A)(i), which includes "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value." 18 U.S.C. § 1030(g), (c)(4)(A)(i)(I). To state a claim under the CFAA, a plaintiff must allege (1) damage or loss, (2) caused by, (3) a violation of one of the substantive provisions in section 1030(a), and (4) conduct involving one of the factors in section 1030(c)(4)(A)(i). *See Dental Health Prods., Inc. v. Ringo*, 2009 WL 1076883, at *6 (E.D. Wis. Apr. 20, 2009) (denying motion to dismiss). The CFAA does not require the plaintiff to identify the particular file or document that the defendant allegedly accessed, or to allege that the defendant lacked permission to copy or transfer the files. *See Mobile Mark, Inc. v. Pakosz*, 2011 WL 3898032, at *2 (N.D. Ill. Sept. 6, 2011) (the

[3] We predict TCS will argue that, because the email chain was not made available for quotation in the Amended Complaint, the Court should ignore it. But, rhetorically speaking, what point would that serve? If for some reason the Court concludes the Amended Complaint needs further facts, Epic would simply seek a stipulation to file a Second Amended Complaint or, absent a stipulation, move the Court for permission to file an amendment. *See* Fed. R. Civ. P. 15(a) ("court should freely give leave when justice so requires"); *Foman v. Davis*, 371 U.S. 178, 182 (1962) (emphasizing same).

complaint sufficiently specified the date and time that the unauthorized activity took place, even though specific documents were not identified).

As Epic properly alleges in the Amended Complaint, TCS violated CFAA Sections 1030(a)(2) and (a)(6), and thereby caused damage or loss to Epic greater than $5,000 during a one-year period.[4] Am. Compl. ¶¶ 50, 70-74.

1. Epic Sufficiently Alleges that TCS Violated CFAA Section 1030(a)(2)(C).

Section 1030(a)(2)(C) prohibits TCS from "intentionally access[ing] a computer without authorization or *exceed[ing] authorized access*, and thereby obtain[ing] . . . information from a[] protected computer." (Emphasis added.)[5] TCS argues that Epic failed to state a claim under section 1030(a)(2)(C) because the CFAA does not apply to the conduct at issue, and because Epic's claim that TCS was not authorized to access the documents at issue is implausible. These arguments fail for the following reasons.

a. The CFAA Applies to the Conduct Alleged in the Complaint.

Section 1030(a)(2) of the CFAA applies when a defendant accesses a computer "without authorization," or by "exceed[ing] authorized access." Exceeding authorization is defined as "access[ing] a computer with authorization and . . . us[ing] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." CFAA § 1030(e)(6). The Seventh Circuit has broadly interpreted the CFAA to permit application of the statute to persons acting outside the scope of their authorization, *i.e.*, based on misuses of computer data in violation of use restrictions.

[4] TCS does not dispute that Epic's alleged damage or loss was caused by TCS or included "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value."

[5] TCS does not dispute that it "obtained information" from a "protected computer."

In particular, in *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006), the Seventh Circuit held that an employee's authorization to access a protected computer terminated when he made the decision to destroy files that were the property of his employer. *Id.* at 420. The employee's "breach of his duty of loyalty terminated his agency relationship . . . and with it his authority to access the laptop, because the only basis of his authority had been that relationship." *Id.* at 420-21; *see also LKQ Corp. v. Thrasher*, 785 F. Supp. 2d 737, 745 (N.D. Ill. 2011) (plaintiff's "allegations of a breach of duty are enough to properly allege that Thrasher lost his authorization to access his company computer"); *Landmark Credit Union v. Doberstein*, 746 F. Supp. 2d 990, 995 (E.D. Wis. 2010) (defendant's "authorization to access the computer in question is a product of the scope of her duties to Landmark under Wisconsin law"); *Dental Health Prods., Inc. v. Ringo*, 2009 WL 1076883, at *7 (E.D. Wis. Apr. 20, 2009) (recognizing that *Citrin* stands for the proposition that an employee who "acquires an interest adverse to his employer and fails to disclose it loses his authority to obtain confidential information"); *Motorola, Inc. v. Lemko Corp.*, 609 F. Supp. 2d 760, 768 (N.D. Ill. 2009) (denying motion to dismiss CFAA claim alleging that employee accessed computers and sent non-employee confidential information from those computers).

Citrin applies even if the unauthorized user is not a direct employee. *See Ocean Tomo, LLC v. Barney*, 2014 WL 2619505, at *5 (N.D. Ill. June 12, 2014) ("[T]he authorization inquiry turns in part on the parties' license agreement, which specifies under which conditions Ocean Tomo may access PatentRating's confidential information."); *see also eBay Inc. v. Digital Point Solutions, Inc.*, 608 F. Supp. 2d 1156, 1164 (N.D. Cal. 2009) ("Allegations with respect to access and use beyond those set forth in a user agreement constitute unauthorized use under the CFAA."); *Therapeutic Research Faculty v. NBTY, Inc.*, 488 F. Supp. 2d 991 (E.D. Cal. 2007) (denying motion to dismiss and finding sufficient allegations that NBTY violated CFAA by entering a single user license agreement, and then sharing the confidential username and passcode among employees). Furthermore, conduct is not authorized, and exceeds authorized access, if the defendant gained access to the information by misrepresenting that he was authorized to access such information. *See TracFone Wireless, Inc. v. Cabrera*, 883 F. Supp. 2d 1220, 1228 (S.D. Fla. 2012). The CFAA applies, therefore, in cases in which the defendant was not authorized to access the information, or where the defendant was acting outside the scope of his or her authorization.[6]

Here, the relevant authorization inquiry is framed by the relationship between Epic and TCS. TCS's access to the UserWeb was subject to the terms of the TCS America Agreement, which included confidentiality provisions and use restrictions, such as limitations on who could use Epic property and how it could be used by TCS. Am. Compl. ¶ 28, 29. Specifically, TCS and its employees were only authorized to access and use Epic information for the limited purpose of facilitating the Kaiser contract. *Id.* ¶ 19. Further, TCS consultants were only permitted access to a limited section of the UserWeb and were required to sign the UserWeb Access Agreement before access was granted. *Id.* ¶¶ 21-23. The UserWeb Access Agreement prohibited consultants from providing their access credentials to third parties, required consultants to keep Epic's information confidential (except to the extent necessary for the Kaiser

[6] TCS relies on *Citrin* and *Landmark* to suggest that the CFAA was intended to cover only hackers and disgruntled employees. Those cases, however, analyze "transmission" and "damages" under section 1030(a)(5)(B), which is not at issue here. *See Citrin*, 440 F.3d at 420; *Landmark*, 746 F. Supp. 2d at 993. In any event, TCS's unauthorized access of Epic's "confidential information on its computer system and distribution of this information" constitutes "hacking." *Charles Schwab & Co. v. Carter*, 2005 WL 351929, at *3 (N.D. Ill. Feb. 11, 2005); *see also Dudick, ex rel. Susquehanna Precision, Inc. v. Vaccarro*, 2007 WL 1847435, at *5 (M.D. Pa. June 25, 2007) ("[T]he CFAA has been held to apply in cases involving former employees wrongfully acquiring and using a plaintiff employer's confidential or trade secret information.").

project), and prohibited consultants from using confidential information for any purpose other than the Kaiser project. *Id.* ¶¶ 21, 23.

With this framework in mind, it is clear that TCS accessed Epic information both without and in excess of its authorization. As described in the Amended Complaint, TCS engaged in a scheme to gain unauthorized access to Epic information. *Id.* ¶ 34. Part of this scheme included using Mr. Gajaram's credentials to access the UserWeb and download over 6,000 documents, including confidential information unnecessary for Mr. Gajaram's Kaiser duties. *Id.* ¶¶ 36, 40. In addition, Mr. Gajaram himself was never properly authorized to access Epic information, since he misrepresented himself as a Kaiser employee to avoid the restrictions in the UserWeb Access Agreement. *Id*. ¶ 42, 44, 45. Because Mr. Gajaram obtained his access through misrepresentation, that access was *per se* unauthorized. *See TracFone Wireless*, 883 F. Supp. 2d at 1228.

Furthermore, even if Mr. Gajaram had been properly authorized to access the UserWeb, Epic alleges that his access (and the access of those to whom he provided his credentials) was in violation of the TCS America Agreement (discussed below), and therefore was "without authorization."[7] *See Citrin*, 440 F.3d 418, 420; *eBay*, 608 F. Supp. 2d at 1164 (access beyond that allowed in user agreement was unauthorized).

In short, "because the only basis of [TCS's] authority [was its] relationship" with Epic, breaching the TCS America Agreement terminated TCS authority to access Epic's UserWeb. *Citrin*, 440 F.3d at 420-21; *Ocean Tomo*, 2014 WL 2619505, at *5.

[7] But for the misrepresentation, Mr. Gajaram would have received the more limited consultant-level access to Epic information. Am. Compl. ¶ 23. The scope of his authority would have been defined by the UserWeb Access Agreement and the TCS America Agreement (*see id.* ¶¶ 21-22, 27-30), both of which he violated.

b. Epic Plausibly Alleges that TCS was Not Authorized to Access the Documents at Issue.

Epic sufficiently alleges that, as prohibited by CFAA section 1030(a)(2)(C), TCS accessed Epic information without or in excess of authorization, and obtained information from a protected computer. The crux of TCS's argument to the contrary is that TCS employees had "broad" access to Epic information pursuant to the TCS America Agreement. This argument misses the point. However described, TCS exceeded the access its personnel were granted.

As explained above, Mr. Gajaram was never properly authorized to access Epic's UserWeb in the first place. As a result, all of Mr. Gajaram's access was without authorization. *See TracFone Wireless, Inc. v. Cabrera*, 883 F. Supp. 2d 1220, 1228 (S.D. Fla. 2012). And the TCS employees who accessed Epic information in India using Mr. Gajaram's credentials accessed that information without authorization as well. Am. Compl. ¶ 37.

Even assuming Mr. Gajaram was authorized to access the UserWeb with proper disclosure of his true identity, he was restrained by the TCS America Agreement, which limited TCS employees' access to Epic training programs for the sole purpose of providing consulting services to Kaiser related to the implementation of Epic property. *Id.* ¶ 27. In particular, the agreement required TCS to: (i) limit access to Epic property to those who *must have* access to implement the property on Kaiser's or Epic's behalf; (ii) use the property only for purposes of in-house training and to assist Kaiser in the implementation of the property; (iii) require its employees to execute a written agreement requiring non-disclosure and limiting the use of confidential information; (iv) use confidential information only for purposes of implementing the property on Kaiser's behalf; (v) notify Epic of any person accessing property without authorization; and (vi) prohibit employees with access to the property from participating in the development or design of competing software, among others. *Id.* ¶ 29.

TCS's and Mr. Gajaram's access exceeded the scope of their authority under the TCS America Agreement in numerous ways. For example, Mr. Gajaram provided his access credentials to persons in India, who did not need to access Epic property to support Kaiser. *Id.* ¶¶ 34-36, 42. The downloaded information included Epic property and confidential information that Mr. Gajaram did not need to perform his own job functions in support of Kaiser. *Id.* ¶¶ 35-36, 39-40. TCS leaders were aware of this scheme and did not put a stop to it or even inform Epic that it was taking place. *Id.* ¶ 33.

Because Epic has sufficiently alleged that TCS intentionally accessed a computer without authorization or by exceeding authorization and thereby obtained Epic information, Epic has sufficiently alleged that TCS violated CFAA § 1030(a)(2)(C).

2. Epic Sufficiently Alleges that TCS Violated CFAA Section 1030(a)(6).

Epic sufficiently alleges that, as prohibited by CFAA section 1030(a)(2)(C), TCS "knowingly and with intent to defraud traffic[ked] . . . in any password or similar information through which a computer may be accessed without authorization [and] such trafficking affect[ed] interstate or foreign commerce." CFAA § 1030(a)(6)(A). TCS argues that Epic fails to state a claim because the CFAA does not apply to the conduct at issue, and because Epic fails to plead an intent to defraud. TCS is wrong on both counts.

a. The CFAA Applies to the Conduct Alleged in the Amended Complaint.

Section 1030(a)(6) prohibits trafficking, which is defined as to "transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of." CFAA § 1029(e)(5). Mr. Gajaram transferred his access credentials to at least two other TCS employees who were not authorized to use those credentials, and thus "traffic[ked]" in those access credentials (i.e., passwords). *Id.*; Am. Compl. ¶ 38.

In addition, Epic has sufficiently alleged that "such trafficking affect[ed] interstate or foreign commerce." Mr. Gajaram, who was located in Oregon, transferred his access credentials to TCS employees who were located in India, and Mr. Gajaram's credentials were used to access the UserWeb from an IP address in India by someone other than Mr. Gajaram. Am. Compl. ¶¶ 37, 38; *see Mobile Mark, Inc. v. Pakosz*, 2011 WL 3898032, at *3 (N.D. Ill. Sept. 6, 2011) (allegations "involved interstate commerce" when plaintiff was located in Illinois, another party was located in Florida, and defendant's bad acts involved accessing computers and obtaining information in Illinois and turning it over to a third party in Florida); *see also Spring Solutions Inc. v. Pac. Cellupage Inc.*, 2014 WL 3715122, at *4 n.2 (July 21, 2014) (noting that allegations under section 1030(a)(6) were sufficient because the complaint alleged that unlocking a telephone involved hacking into and gaining access to the Sprint networks, and that the process of trafficking in mobile phones included sharing confidential codes and passwords stored on the phones, which were then used to access Sprint's networks). Epic therefore has alleged conduct covered by Section 1030(a)(6).[8]

b. Epic Sufficiently Pleads an Intent to Defraud.

Section 1030(a)(6) prohibits trafficking in passwords if such trafficking is done "knowingly and with intent to defraud."[9] "Intent to defraud" is not the same as and does not implicate the heightened standard required by Rule 9(b). *SKF USA, Inc. v. Bjerkness*, 636 F. Supp. 2d 696, 719 n.13 (N.D. Ill. 2009). "[F]raud under the CFAA only requires a showing of

[8] Notably, TCS's sole argument that Epic did not state a claim under section 1030(a)(6) involves quoting a passage of the legislative history. Mot. at 15-16. TCS makes no effort to explain how the plain language of the statute is unclear, or to cite any cases holding that the CFAA is inapplicable in circumstances such as those alleged here.

[9] Although TCS correctly points out that there are few cases analyzing section 1030(a)(6), it ignores that there are several cases analyzing "intend to defraud" in discussing other CFAA sections. Mot. at 19.

unlawful access; there is no need to plead the elements of common law fraud to state a claim under the Act." *eBay*, 608 F. Supp. 2d 1156. Instead, for purposes of the CFAA, "defraud" "simply means wrongdoing and does not require proof of common law fraud." *Hanger Prosthetics & Orthotics, Inc. v. Capstone Orthopedic, Inc.*, 556 F. Supp. 2d 1122, 1131-32 (E.D. Cal. 2008) (inferring that an intent to defraud turns any use into one exceeding authority). Furthermore, because this is not a fraud claim, at the pleading stage detailed factual allegations are not required, and "intent to defraud" may be alleged generally. *Dental Health Prods., Inc. v. Ringo*, 2009 WL 1076883, at *8 (E.D. Wis. Apr. 20, 2009).

Epic sufficiently alleges an intent to defraud. As stated in the Amended Complaint, Mr. Gajaram obtained his access credentials in a fraudulent manner by misrepresenting that he was a "customer employee" when registering for his credentials and, after his credentials were suspended upon discovery of the fraudulent access, again attempting to hide his position as a TCS consultant. Am. Compl. ¶¶ 41-44. Also, while Mr. Gajaram knew that he could not provide his access credentials to other people (Am. Compl. ¶ 21 (UserWeb Access Agreement provision)), he nevertheless knowingly and wrongfully provided those credentials to at least two other TCS personnel who were otherwise unauthorized to access Epic information. *Id.* ¶¶ 38, 47-48. TCS leaders were aware of and complicit in this scheme, and Mr. Gajaram's credentials were used to download documents from an IP address in India registered to TCS. *Id.*¶¶ 34, 37.

These allegations are more than sufficient to satisfy the generalized pleading required, and Epic therefore has sufficiently alleged that TCS violated Section 1030(a)(6).

3. Epic Adequately Pleads Damages or Loss.

A plaintiff alleging a CFAA claim must establish either "damage *or* loss," but not both. CFAA § 1030(g); *Pascal Pour Elle, Ltd. v. Jim*, --- F. Supp. 3d ---, 2014 WL 6980699, at *6

(N.D. Ill. 2014); *Navistar, Inc. v. New Baltimore Garage, Inc.*, 2012 WL 4338816, at *6 (N.D. Ill. Sept. 20, 2012).[10] In other words, it is enough if the plaintiff alleges that it sustained a loss, "even if data or computers were not damaged," so long as the plaintiff suffers a loss that "qualifies under the statute." *1st Rate Mortg. Corp. v. Vision Mortg. Servs. Corp.*, 2011 WL 666088, at *2 (E.D. Wis. Feb. 15, 2011). Under the CRAA, "'loss' means *any reasonable cost* to any victim, *including the cost of responding to an offense*, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." CFAA § 1030(e)(8), (11) (emphasis added).

As courts in this circuit have held, costs associated with security assessments and investigating the extent of unauthorized access to a computer or network constitute "loss" under the CFAA. *Pascal Pour*, 2014 WL 6980699, at *7 (denying motion to dismiss because loss allegation — "over $5000 in investigation and security assessment costs" — was sufficient); *Navistar, Inc. v. New Baltimore Garage, Inc.*, 2012 WL 4338816, at *8 (N.D. Ill. Sept. 20, 2012) (same); *Mobile Mark*, 2011 WL 3898032 (complaint sufficiently alleged "loss" in that plaintiff was "forced to perform a forensic computer analysis" to investigate defendant's alleged wrongdoing and also "suffered a loss of customers, goodwill, sales, and business opportunities"); *Dental Health Prods., Inc. v. Ringo*, 2011 WL 3793961, at *3 (E.D. Wis. Aug. 25, 2011) (same). This is true even if the court ultimately determines that the alleged offense caused no damage as defined by the CFAA. *Navistar*, 2012 WL 4338816, at *8. Also, the unauthorized

[10] Although TCS cites some district court decisions that evidence a split as to whether CFAA requires damage *and* loss or damage *or* loss, the Seventh Circuit has not yet spoken on the issue and the statute is clearly written in the disjunctive. *See* Mot. at 16-19; CFAA § 1030(g). As a result, the Court should follow those well-reasoned cases holding that a finding of damage *or* loss is sufficient to state a claim under the CFAA.

access and disclosure of information "may constitute an impairment to the integrity of data or information, even though no data was physically changed or erased." *Therapeutic Research Faculty v. NBTY, Inc.*, 488 F. Supp. 2d at 996-97 (deeming sufficient an allegation that a loss was suffered because full corporate license cost approximately forty thousand dollars per year, whereas defendant purchased only $100 single-user subscription).

Epic has sufficiently alleged a loss under the statute. Epic has incurred substantial sums, in excess of $5,000, in costs and losses related to investigating TCS's unauthorized access to Epic's UserWeb. Am. Compl. ¶ 50. Epic will continue to incur losses as the investigation continues. *Id.* In addition, because Epic is still investigating the misconduct of TCS personnel, it does not yet know the extent of any damage caused by that misconduct. *Id.* ¶ 48.

B. <u>Epic States a Claim under the Wisconsin Computer Crimes Act.</u>

The Wisconsin Computer Crimes Act provides that "[w]hoever willfully, knowingly and without authorization does any of the following may be penalized . . . ."[11] Wis. Stat. § 943.70(2)(a). The enumerated violations include accessing, copying, and taking possession of programs or supporting documentation, as well as disclosing restricted access codes and other restricted access information to unauthorized persons.

Unlike the CFAA, in which "without authorization" modifies "access" in every subsection, under the Computer Crimes Act, "without authorization" modifies *each act*, not just access. *Compare* 18 U.S.C. § 1030(a) (tying authorization to access), *with* Wis. Stat. § 943.70(2)(a). Thus, the statute prohibits copying data without authorization, disclosing restricted access codes without authorization, and, of course, accessing information without authorization, among others. If a defendant is authorized to access information, but not to destroy it, for

[11] TCS does not dispute that its access to Epic's information was willful and knowing.

example, that destruction is still a violation of the statute. *See Priority Int'l Animal Concepts, Inc. v. Bryk*, 2012 WL 1854121, at *8 (E.D. Wis. May 21, 2012) ("The fact that Gleisner obtained the data with authorization does not defeat the claim.").

As explained above, TCS accessed, copied, and took possession of Epic data and programs, all without or in excess of authorization, because Mr. Gajaram (i) obtained access via misrepresentation, (ii) exceeded any access he would have been provided but for that misrepresentation, and (iii) violated the terms of the TCS America Agreement. TCS does not dispute that TCS copied and took possession of Epic data without authorization. Mot. at 23 (arguing only that TCS was authorized to access Epic information). Also, Mr. Gajaram provided his restricted access credentials to unauthorized persons without authorization. Am. Compl. ¶¶ 37-38, 47-48. TCS does not dispute this either.

TCS thus violated the Computer Crimes Act, and Epic is entitled to injunctive relief and money damages in an amount to be determined. Although Wisconsin courts typically grant injunctive relief for violations of the Act, money damages are also proper.[12] This is supported by other sections of the statute, including section 943.70(a), which defines data as "property." Because tort law typically provides monetary remedies for intentional, nonconsensual, and harmful interference with another's property, it is logical to assume that monetary remedies are appropriate in this case. *See* Michael McChrystan, William Gleisner, III & Michael Kuborn, *Invasions of Computer Privacy*, Wisconsin Lawyer, 71-OCT WILAW 25 (Oct. 1998).

[12] At least one Wisconsin court has recognized that this issue has not been definitively decided. *See Liturgical Publications, Inc. v. Karides*, 2006 WL 931892, 715 N.W. 2d 240, at *15 n.6 (Table) (Wis. App. 2006) (noting that the issue remains of whether money damages are an available remedy for a violation of the Computer Crimes Act).

C. Epic Sufficiently Alleges Misappropriation of Trade Secrets.

TCS argues that Epic's third cause of action for violation of Wisconsin's Uniform Trade Secrets Act, Wis. Stat. § 134.90 (the "WUTSA"), fails as a matter of law because Epic does not sufficiently allege misappropriation, and Epic's supposedly vague allegations do not put TCS on fair notice of the information Epic contends constitutes trade secrets. However, TCS's argument depends on discrediting the detailed allegations set forth in the Amended Complaint, rather than taking those allegations as true. The argument is also premature at the pleading stage.

1. Epic Alleges Sufficient Facts Concerning Misappropriation.

TCS contends Epic failed to plead misappropriation under either section 134.90(2)(a) or 134.90(2)(b) of the WUTSA. Mot. at 23-24. TCS is wrong on both counts.

Section 134.90(2)(a) provides that "[n]o person, including the state, may misappropriate or threaten to misappropriate a trade secret by . . . [a]cquiring the trade secret of another by means which the person knows or has reason to know constitute *improper means*." Wis. Stat. § 134.90(2)(a) (emphasis added). TCS argues that Epic cannot plausibly allege that TCS obtained the documents by "improper means," which is defined by section 134.90(1)(a) to include "espionage, theft, bribery, misrepresentation and breach or inducement of a breach of duty to maintain secrecy." Mot. at 24-25. Wis. Stat. § 134.90(1)(a). In particular, TCS argues: "Epic itself alleges that TCS obtained the information by logging in to UserWeb," it cannot "plausibly allege improper means." Mot. at 25.

TCS's argument is defeated by the allegations in the Amended Complaint. Epic alleges that although UserWeb access is limited to those who require information to service an Epic customer, Am. Compl. ¶ 19, TCS personnel fraudulently accessed the UserWeb and used the information obtained "to benefit [TCS's] competing Med Mantra software," *id.* ¶ 33. TCS exceeded any authority it initially had to access the UserWeb when it defrauded Epic to obtain information for its competitive product. Thus, TCS knowingly used "improper means" to acquire Epic's trade secret information.

With respect to section 134.90(2)(b), TCS argues that Epic has not plausibly alleged that TCS used Epic's trade secret information. Section 134.90(2)(b) provides, in relevant part:

> No person . . . may misappropriate or threaten to misappropriate a trade secret by . . . [d]isclosing or using without express or implied consent a trade secret of another if the person did any of the following:
>
> 1. Used improper means to acquire knowledge of the trade secret.
>
> 2. At the time of disclosure or use, knew or had reason to know that he or she obtained knowledge of the trade secret through any of the following means:
>
> > a. Deriving it from or through a person who utilized improper means to acquire it.
> >
> > b. Acquiring it under circumstances giving rise to a duty to maintain its secrecy or limit its use.

Wis. Stat. § 134.90(2)(b). As TCS acknowledges, the Amended Complaint alleges that Epic learned from Mr. Guionnet that TCS used information obtained from Epic's UserWeb "to benefit its competing Med Mantra software." Mot. 25. TCS further acknowledges that Epic alleges that TCS sought "to use information and documents related to Epic's leading software to benefit TCS's creation of and improvements to TCS's competing Med Mantra product." *Id.* Rather than address these allegations, however, TCS attacks the source of Epic's information, Mr. Guionnet. Mot. 26. As discussed above, other than its attacks on Mr. Guionnet's credibility, TCS provides no basis on which to discredit Mr. Guionnet's first-hand information, which has been corroborated by independent investigation. TCS cannot successfully argue that Epic has failed to plead misappropriation under section 134.90(2)(b).

2. TCS's Argument that Epic Fails to Allege the Existence of Trade Secrets is Premature on a Motion to Dismiss.

TCS also argues that Epic's allegations "are nothing more than legal conclusions" that "fail to allege the ultimate facts showing the existence of a trade secret." Mot. at 27. However, "[e]ven post-*Iqbal*, the plaintiff in pleading is not required to provide 'detailed factual allegations.' Rather, a plaintiff, through the complaint, must provide notice to the defendants of the claims alleged against them." *Radiator Exp. Warehouse, Inc. v. Shie*, 708 F. Supp. 2d 762, 767 (E.D. Wis. 2010); *see also Bissessur v. Ind. Univ. Bd. of Trustees.*, 581 F.3d 599, 602 (7th Cir. 2009).

To determine whether information meets the statutory definition of a trade secret, the court must engage in a "fact-intensive" inquiry considering a variety of factors, such as: "(1) the extent to which the information is known outside the business, (2) the extent to which it is known by employees and others involved in the business, (3) the extent of measures taken to guard the secrecy of the information, (4) the value of the information to the business and its competitors, (5) the amount of effort or money expended by the business in developing the information; and (6) the ease or difficulty with which the information could be properly acquired or duplicated by others." *Radiator*, 708 F. Supp. 2d at 766-67; *Genzyme Corp. v. Bishop*, 463 F. Supp. 2d 946, 949 (W.D. Wis. 2006).

As many courts have found, such a fact-intensive determination is more appropriate at the summary judgment stage. *See Radiator*, 708 F. Supp. 2d at 767 n.6 (noting the court could not find a single case granting a motion to dismiss a WUTSA claim because the information at issue did not constitute a "trade secret"); *Genzyme Corp.*, 463 F. Supp. 2d at 949 (denying motion to dismiss because the court did not "possess sufficient factual information to conclude as a matter of law that the allegedly received and retained information . . . constitutes a trade secret," and recognizing the inquiry is better addressed on summary judgment). Indeed, TCS relies heavily on *ECT Int'l, Inc. v. Zwerlein*, 228 Wis. 2d 343 (Wis. App. 1999), which involved a motion for summary judgment rather than a motion to dismiss. In fact, most of the decisions on which TCS relies were decided on a motion for summary judgment. *E.g.*, *Lands' End, Inc. v. Genesys Software Sys., Inc.*, No. 13-CV-38-BBC, 2014 WL 266630 (W.D. Wis. Jan. 24, 2014); *Fail-Safe LLC v. A.O. Smith Corp.*, 744 F. Supp. 2d 831 (E.D. Wis. 2010).

Regardless, even if TCS's argument was appropriate on a motion to dismiss, Epic's allegations are sufficient to allege a viable claim. The Amended Complaint alleges that the documents downloaded by TCS personnel included trade secret documents detailing over twenty years of development of Epic's proprietary software and database systems, including documents that decode the operation of its source code that would otherwise be unusable to those outside of Epic and information regarding Epic's system capabilities and functions. Am. Compl. ¶ 39. Epic alleges that all of this information would "reveal decades of Epic's work with its customers to determine the functionality desirable or required for Epic to provide successful products to those customers." *Id.* As discussed above, Epic has also alleged that it took reasonable measures to maintain the secrecy of its trade secret information, including requiring written agreements regarding the confidentiality of such information before allowing even limited access to Epic's UserWeb. *Id.* ¶¶ 19-24.

Accordingly, Epic has alleged sufficient facts to show that its trade secret information is valuable and conveyed under an assumption of secrecy. *See, e.g.*, *Radiator*, 708 F. Supp. 2d at 767 (allegations that information included core business strategies was "far from threadbare," and alleged basis for credible claim that the information was highly valuable and conveyed under an assumption of secrecy); *see also BondPro Corp. v. Siemens Westinghouse Power Corp.*, 320

F. Supp. 2d 804, 806-07 (W.D. Wis. 2004) (denying motion to dismiss trade secrets claim where plaintiff alleged that documents disclosed to defendant were stamped "proprietary statement" and contained trade secrets for which plaintiff owned all of the intellectual property). Epic's allegations are more than sufficient to allow TCS to frame an answer. If TCS requires more specificity regarding Epic's trade secret information, TCS can obtain that information through discovery. *See Radiator*, 708 F. Supp. 2d at 767 (allegations found plausible even though "facts may arise during discovery that cast doubts on the plaintiff's allegations").

3. Epic Alleges Sufficient Facts Concerning Its Efforts to Protect its Trade Secret Information.

TCS contends that Epic's trade secret misappropriation claim also fails because Epic does not allege any facts concerning its efforts to keep its documents on UserWeb secret. TCS's argument hinges on the fact that Epic authorized TCS to access UserWeb pursuant to the TCS America Agreement. Mot. at 30. This nonsensical argument appears to be that, because Epic and TCS were competitors, Epic did not take adequate safeguards to protect its information, even though it required TCS to enter into a written agreement limiting its access to UserWeb for the express purpose of supporting Epic's contract with Kaiser. Am. Compl. ¶ 29. TCS's argument is essentially an admission that TCS could not be trusted to abide by its agreements with Epic, which falls far short of establishing that Epic failed to make efforts to keep its documents secret.

Moreover, it is well-established that limited disclosure of trade secret information does not forfeit trade secret protection. In *Centrifugal Acquisition Corp., Inc. v. Moon*, 849 F. Supp. 2d 814, 834 (E.D. Wis. 2012), for example, the defendants argued that the plaintiff's allegedly proprietary process was not a trade secret "because certain aspects of the process were disclosed to various employees and contractors on a 'need to know' basis." *Id.* However, the court held that the disclosure of trade secrets to a "limited number of outsiders for a particular purpose" does not forfeit trade secret protection. *Id.* (citing *Rockwell Graphic Sys., Inc. v. DEV Indus., Inc.*, 925 F.2d 174, 177 (7th Cir. 1991)). "On the contrary, such disclosure, which is often necessary to the efficient exploitation of a trade secret, imposes a duty of confidentiality on the part of the person to whom the disclosure is made." *Id.* Also, the court explained that "there is an important distinction between disclosing the entire process and disclosing a discrete component thereof." *Id.* Here, Epic alleged that it provided limited access to a discrete set of documents on UserWeb, subject to strict confidentiality agreements. It is indisputable that Epic's trade secret information was "subject to reasonable efforts to maintain secrecy." *See id.*

In fact, Epic has taken steps to protect its information above and beyond those necessary under Wisconsin law, which does not even require express, written contracts of confidentiality. Pursuant to the WUTSA, "an implied undertaking to abide by the trade's norms of confidentiality suffices." *Id.* (citing *Hicklin Eng., L.C. v. Bartell*, 439 F.3d 346, 350 (7th Cir. 2006)) (finding it was reasonable for the plaintiff to assume that the defendant would maintain the secrecy of alleged trade secrets even without a confidentiality agreement). Indeed, in a case cited by TCS, *Fail–Safe LLC v. A.O. Smith Corp.*, 744 F. Supp. 2d 831, 859-60 (E.D. Wis. 2010), the court recognized that an implied obligation of confidentiality can arise when "the person knew or had reason to know that the disclosure was intended to be in confidence" and "the other party to the disclosure was reasonable in inferring that the person consented to an obligation of confidentiality." *Id.* at 859. The "question posed is whether under the circumstances, the recipient of the information knew or should have known that the information is a trade secret and that the disclosure was made in confidence." *Id.* (citing *RTE Corp. v. Coatings, Inc.*, 84 Wis. 2d 105, 117-18 (1978)). Thus, even if Epic had not required binding confidentiality agreements, it has alleged sufficient facts to show that as consultants for Kaiser, TCS and its employees knew or should have known that the information constituted trade secrets and that Epic's disclosure was made in confidence. Am. Compl. ¶¶ 25-32.

D. **Epic States a Claim for Breach of Contract.**

To state a claim for breach of contract under Wisconsin law, Epic must plead "(1) the existence of a contract creating obligations flowing from [TCS] to [Epic]; (2) a breach of those obligations; and (3) damages arising from the breach." *Apple, Inc. v. Motorola Mobility, Inc.*, No. 11-178, 2011 WL 7324582, at *8 (W.D. Wis. June 7, 2011). Notice pleading requires only that Epic allege "facts sufficient to show that the case is plausible." *Hedeen Int'l, LLC v. OzWest, Inc*., No. 14-304, 2014 WL 5682507, at *1 (E.D. Wis. Nov. 4, 2014). Epic is not even required to plead specific legal theories. It is sufficient if "the gist of the complaint can readily be discerned." *Id.* (allegations suggesting "both that a contract existed and that the Defendants violated that contract by not paying royalties" were "enough to at least survive a motion to dismiss," even when no specific causes of action were alleged).

Here, TCS argues that Epic has failed to plead a breach of contract because: (i) Epic does not "point to any particular provision of the Agreement that it contends TCS has breached;" (ii) "Epic's allegations that TCS employees wrongfully obtained access to UserWeb and sent documents to other TCS employees in India 'for purposes other than' work on Kaiser's behalf are wholly conclusory;" and (iii) "Epic's allegation that TCS breached the TCS-Epic Agreement by using Epic information in connection with Med Mantra is based entirely on the assertions of Mr. Guionnet." Mot. at 31-32. These arguments do not work.

First, Epic sets forth all of the relevant provisions of the TCS America Agreement in paragraphs 27-30 of the Amended Complaint, which are incorporated by reference into the fourth cause of action for breach of contract. Am. Compl. ¶ 90. Epic alleges that "[t]he TCS

America Agreement is a valid agreement under which TCS America, acting as the agent and alter ego of TCS India, made certain promises that, while consulting for Kaiser, TCS America would protect Epic's confidential and proprietary information, including by restricting access to the information, limiting its use to training and other consulting activities for Epic customers, and preventing use of the information to design, develop, or enhance a competing software product." Am. Compl. ¶ 91. These allegations are more than sufficient to put TCS on notice of the provisions of the agreement that Epic contends were breached by TCS.

Second, Epic adequately alleges that TCS breached the TCS America Agreement when it "improperly utilize[ed] UserWeb access credentials through non-registered employees and employees who do not require access to consult for an Epic customer" and "sen[t] that information to India for purposes other than implementing the Program Property on Epic's or its customer's behalf." Am. Compl. ¶ 94. Specifically, Epic has alleged that "Mr. Gajaram's credentials were used to download documents from IP addresses in India registered to TCS — meaning that someone else within TCS, but outside the Kaiser network, used Mr. Gajaram's login credentials as if they were Mr. Gajaram." *Id.* ¶ 37. Epic also alleges that neither of the TCS employees who used Mr. Gajaram's credentials "were authorized to use those credentials or had received permission or any authorization to take Epic information from Epic's UserWeb, and neither needed the information in connection with the implementation of Epic's Program Property for Kaiser." *Id.* ¶ 38. Epic provides examples of the types of downloaded documents that "were not even required for Mr. Gajaram to perform his own job functions in support of Kaiser," (*id.* ¶ 40), and alleges that Mr. Gajaram himself "admitted that these other TCS personnel did not need access to the Epic UserWeb," *id.* ¶ 47.

TCS argues that the TCS America Agreement makes "no mention of needing a UserWeb Access Agreement for each individual employee who is provided access." Mot. at 31. Even if true, this fact is irrelevant. As alleged in the Amended Complaint, the TCS America Agreement obligates TCS to "limit access to the Program Property to those [TCS employees] who must have access to the Program Property in order to implement the Program Property [which is defined broadly as 'the Documentation for all of Epic's computer programs' (*see* Am. Compl. ¶ 28)], on Epic's or its customer's behalf" (i.e., Kaiser). Am. Compl. ¶ 29(a). The allegation that Mr. Gajaram downloaded Epic Program Property he did not need for servicing the Kaiser account, along with Mr. Gajaram's admission that he shared such Program Property with TCS employees who did not need such information to service the Kaiser account, suffice to state a claim for breach of the TCS America Agreement.

Third, Epic adequately alleges that TCS breached the TCS America Agreement by "using Epic's confidential and proprietary information — including Program Property, Confidential Information, and Documentation — to develop and enhance Defendants' software designed to compete with Epic products." Am. Compl. ¶ 94. TCS argues that Epic cannot rely on Mr. Guionnet for these allegations. Mot. at 32. As discussed above, Epic has provided sufficient facts to support the plausibility of Mr. Guionnet's information, which has been corroborated by independent investigation. TCS also cites to *Maclean-Fogg Co. v. Edge Composites, L.L.C.*, No. 08-6367, 2009 WL 1010426 (N.D. Ill. Apr. 14, 2009), for the proposition that Epic cannot rely on allegations "made on information and belief." Mot. at 32. Yet *Maclean-Fogg* is easily distinguishable, as in that case "Plaintiffs d[id] not state *any grounds* for their suspicion" that the defendant had disclosed trade secrets in violation of his confidentiality agreement. *Id.* at *6 (emphasis added). In fact, the court noted that allegations based exclusively on information and belief would be sufficient when "the facts are inaccessible to the pleader, and there is a reasonable basis to suspect the facts are true." *Id.*

Here, in addition to the information provided by Mr. Guionnet, Epic has engaged in an independent analysis that revealed TCS's unauthorized downloading and sharing of thousands of Epic documents with various TCS personnel admittedly unrelated to the Kaiser account. Am. Compl. ¶ 36. Epic cannot confirm without discovery exactly what TCS has done with that information, as those facts are "inaccessible to the pleader" and in TCS's possession alone. But the allegations in the Amended Complaint provide much more than a "reasonable basis to suspect" that TCS was doing exactly what Mr. Guionnet has indicated — using Epic's confidential information to improve its own competitive Med Mantra software.

E. <u>Epic States a Claim for Breach of the Implied Covenant of Good Faith and Fair Dealing.</u>

The Wisconsin Supreme Court has recognized that "[e]very contract implies good faith and fair dealing between the parties to it." *In re Chayka's Estate*, 47 Wis. 2d 102, 107 (Wis. 1970). "A party breaches the duty of good faith and fair dealing when it technically complies with the terms of a contract but engages in conduct such as 'evasion of the spirit of the bargain, lack of diligence and slacking off, willful rendering of imperfect performance, abuse of power to specify terms, and interference with or failure to cooperate in the other party's performance.'" *Latino Food Marketers, LLC v. Ole Mexican Foods, Inc.*, No. 03-0190, 2004 WL 632869, at *2 (W.D. Wis. Mar. 29, 2004) (quoting *Foseid v. State Bank of Cross Plains*, 197 Wis. 2d 772, 797 (Wis. Ct. App. 1995); *see also Bozzacchi v. O'Malley*, 211 Wis. 2d 622, 626 (Wis. App. Ct. 1997) (relying on *Chayka* and holding that "[t]he Bozzacchis' crabbed reading of the requirement that they 'rent' the Spindle Top Court property for $650 per month does not comport with this duty of good-faith performance"); *Kreckel v. Walbridge Aldinger Co.*, 295

Wis. 2d 649, 662 (Wis. App. Ct. 2006) ("A party can be liable for breach of the implied covenant of good faith even though all the terms of the written agreement may have been fulfilled." (internal quotation marks omitted)).

In *Chayka*, a husband and wife executed a will giving the property to the survivor, and providing that on the survivor's death the property should go to a named third party. 47 Wis. 2d at 105. After the husband died, the wife gave most of the property to her second husband, leaving little for disposition to the third person. *Id.* The court held that "[w]hat [the wife] in fact has done has stripped nearly all of the flesh from the bones [of the agreement], leaving only a skeleton for testamentary disposition to [the third party]. This is a compliance in form, not in substance, that breaches the covenant of good faith that accompanies every contract, by accomplishing exactly what the agreement of the parties sought to prevent." *Id.* at 107.

Here, Epic alleges that, through "the intentional and deceitful conduct alleged above, Defendants breached the covenant of good faith and fair dealing implied in the TCS America Agreement and denied Epic benefits due to Epic under the agreement." Am. Compl. ¶ 101. "Even assuming these actions did not violate the express terms of the TCS America Agreement, Defendants' conduct violated the spirit of the TCS America Agreement, and deprived Epic of the fruits of that contract, by accomplishing exactly what the agreement of the parties sought to prevent." *Id.* ¶ 102. In short, whether or not TCS breached the express terms of the agreement between the parties, TCS' actions have "accomplish[ed] exactly what the agreement of the parties sought to prevent." *Chayka*, 47 Wis.2d at 107.

TCS argues that "Wisconsin does not recognize the implied covenant as a cause of action separate and apart from a breach of contract claim." Mot. at 32. Yet the two cases TCS cites for this proposition — *Gilson v. Rainin Instrument, LLC*, No. 04-852, 2005 WL 955251 (W.D. Wis.

Apr. 25, 2005) and *Alliance Laundry Systems LLC v. Eaton Corp.*, No. 13-687, 2013 WL 5719011 (E.D. Wis. Oct. 21, 2013) — are inapposite, as they both interpret the "obligation of good faith" provision in section 401.304 (formerly section 401.203) of the Wisconsin Uniform Commercial Code, which is irrelevant to Epic's common law claim for breach of the implied covenant. That UCC provision provides that "[e]very contract or duty within [the Wisconsin UCC] imposes an obligation of good faith in its performance or enforcement," and the Wisconsin Court of Appeals has held that this section "does not support an independent cause of action for failure to act in good faith under a contract." *Hauer v. Union State Bank of Wautoma*, 192 Wis. 2d 576, 596-97 (Ct. App. 1995). Both *Gilson* and *Alliance* rely on *Hauer* in finding no independent cause of action for the implied duty of good faith claim at issue. *See Gilson*, 2005 WL 955251, at *8; *Alliance*, 2013 WL 5719011, at *5. However, because the UCC applies only to "transactions in goods" (*Gilson*, 2005 WL 955251, at *4), the *Hauer* case — and by extension the cases on which TCS relies — are inapplicable in this matter. Wisconsin courts have clearly recognized an implied covenant cause of action for contracts outside the UCC, such as the TCS America Agreement: "[I]s a breach of the implied duty of good-faith dealing something separate from breach of the terms of the contract? We think it is." *Foseid*, 197 Wis. 2d at 794.

TCS also argues that Epic's good faith claim should be dismissed as "duplicative" of its cause of action for breach of contract. Mot. at 32. However, Epic's claim is expressly pled in the alternative (*see* Am. Compl. ¶ 102), and "plaintiff cites no authority that would prohibit defendant from asserting a bad faith claim in the alternative to its breach of contract claim." *Latino Food Marketers*, 2004 WL 632869, at *2 (denying plaintiff's motion for summary judgment with respect to defendant's claim for breach of the duty of good faith and fair dealing); *see also Maryland Staffing Servs., Inc. v. Manpower, Inc.*, 936 F. Supp. 1494, 1508-09 (E.D.

Wis. 1996) (denying motion to dismiss good faith claim that "overlaps" with the breach of contract claim, although "[i]n all likelihood, these two Counts will constitute alternative claims for relief, permissible pleading under the Federal Rules").

F. **Epic's Tort and State Law Claims are Not Preempted by the WUTSA.**

TCS contends that Epic's tort claims and statutory claims under Wisconsin law are preempted by the WUTSA and should be dismissed. In particular, TCS argues that Epic's claims are all based on the following set of facts: "TCS allegedly accessing Epic's trade secrets through User Web, and then using those trade secrets in connection with the development of TCS's allegedly competing product, Med Mantra." Mot. at 33.

The WUTSA displaces tort claims based on misappropriation of a trade secret, but does not affect: (i) any contractual claims, whether or not based upon misappropriation of a trade secret; (ii) any civil remedy not based upon misappropriation of a trade secret; or (iii) any criminal remedy, whether or not based upon misappropriation of a trade secret. Wis. Stat. § 134.90(6). Epic's carefully pleaded claims fall into one or more of these three categories.

The Supreme Court of Wisconsin held in *Burbank Grease Servs., LLC v. Sokolowski*, 294 Wis. 2d 274, 298 (2006), that "any civil tort claim not grounded in a trade secret, as defined in the statute, remains available." TCS contends that Epic's reliance on *Burbank* is misplaced because "prior rulings in the case had already determined that none of the information at issue constituted trade secrets, so the court was only dealing with confidential information outside the scope of the UTSA." Mot. at 35. TCS also argues that, because Epic does not specify which information accessed by TCS allegedly constitutes trade secrets and which information allegedly constitutes confidential information not protected by WUTSA, TCS is not on fair notice of Epic's claims. *Id.* Both of these arguments must fail.

1. TCS's Preemption Argument is Premature.

To the extent TCS argues that Epic's claims are preempted because they are based on information that will *ultimately* be determined to be trade secret information, TCS' argument is premature on a motion to dismiss. The fact that the Court has not yet made a determination as to whether Epic's confidential data constitutes trade secret information for purposes of the WUTSA does not provide a basis on which to dismiss Epic's claims as preempted at this stage of the litigation.

For instance, in *Radiator Exp. Warehouse, Inc. v. Shie*, 708 F. Supp. 2d 762, 769 (E.D. Wis. 2010), the plaintiff asserted five causes of action in addition to its misappropriation of trade secrets claim, including intentional misrepresentation and conversion. *Id.* The court rejected defendant's motion to dismiss based on section 134.90(6), as "discovery could prove that the information at issue in the plaintiff's first cause of action [for misappropriation of trade secrets] falls short of the statutory definition of 'trade secret' within the meaning of the WITSA, forcing the plaintiffs to try to recover other civil tort claims not grounded in trade secret." *Id.* (citing *Burbank*). Accordingly, the court declined to dismiss the plaintiff's claims, finding that "a claim of abrogation is premature at the motion to dismiss stage." *Id.* Similarly, in *Genzyme Corp. v. Bishop*, 463 F. Supp. 2d 946, 949 (W.D. Wis. 2006), the court denied the defendant's motion to dismiss the plaintiff's unjust enrichment claim because it did not possess "sufficient factual information to conclude as a matter of law that the allegedly received and retained information . . . constitutes a trade secret." Even if the plaintiff's unjust enrichment claim could ultimately be preempted by the WUTSA, "such an inquiry is better addressed on summary judgment where both parties have the opportunity to develop the record and submit evidence to the Court in support of their respective positions." *Id.*

Here, Epic has provided allegations sufficient to put TCS on notice of its claims, which, as discussed below, are expressly based on non-trade secret information. Regardless, discovery will show that these claims are not grounded in trade secret, and TCS's motion to dismiss based on preemption is therefore premature at this stage of the litigation.

2. Epic's Claims are Not Grounded in Trade Secret.

As in *Burbank*, Epic's other claims are expressly based on non-trade secret information. For example, Epic's second cause of action for violation of the Computer Crimes Act alleges that "Defendants willfully, knowingly, and without authorization accessed, copied, and took possession of *electronic data and information* belonging to Epic . . . from Epic's UserWeb, without Epic's consent and without lawful authority." Am. Compl. ¶ 76. This claim is not tied to any misappropriation of trade secret information. Epic's sixth cause of action for fraud similarly alleges additional facts beyond its misappropriation of trade secrets claim, including the that TCS made intentional misrepresentations "to advance [Defendants'] apparent scheme to steal confidential information, documents, intellectual property, and other information from Epic." *Id.* ¶ 107.

With respect to the remaining claims challenged by TCS, Epic specifically states in the Amended Complaint that each cause of action "is based on Epic's confidential information that does not meet the statutory definition of a trade secret." *Id.* ¶¶ 112, 114, 118, 125, 130, 135 (citing *Burbank*). These causes of action also include the following additional allegations unrelated to the misappropriation of WUTSA trade secrets:

- In its Seventh Cause of Action for conversion, Epic alleges that "Defendants willfully took, controlled, interfered with, and/or deprived Epic of documents and information without Epic's consent and without lawful authority, including information and documents that do not comprise trade secrets." *Id.* at ¶ 114.

- In its Eighth Cause of Action for common law unfair competition, Epic alleges that "Epic has invested substantial time, labor, and money in the creation and development of its data systems, software, documents, and information. Without Epic's authorization, Defendants intentionally and wrongfully used, and will continue to use, Epic's stolen documents, password credentials, and information in unfair competition with Epic." *Id.* at ¶¶ 119-120.

- In its Ninth Cause of Action for injury to business under Wis. Stat. § 134.01, Epic alleges: "Defendants conspired and acted in concert together to misappropriate and misuse Epic's confidential and proprietary information for the purpose of willfully or maliciously injuring Epic's business via competitive harm to Epic's competing software product, including EpicCare Inpatient and EpicCare Ambulatory." *Id.* ¶ 126.

- Epic alleges in its Tenth Cause of Action for property damages or loss under Wis. Stat. § 895.446: "Without Epic's consent, Defendants intentionally took and all Defendants have used property belonging to Epic, including Epic documents and other property found on Epic's UserWeb, with the intent to deprive Epic permanently of the possession, use, and/or value of such property in violation of Wis. Stat. § 943.20." *Id.* ¶ 131.

- In its Eleventh Cause of Action for unjust enrichment, Epic alleges that "Epic was, and is, entitled to the benefit of the data, documents, and information that was stored on its UserWeb. With full knowledge of Epic's rights, Defendants unjustly obtained the benefit of Epic's property, as described herein, resulting in inequity and damage to Epic, as described in more detail above." *Id.* ¶¶ 136-37.

As in *Burbank*, Epic's claims are expressly based on non-trade secret information, and TCS's preemption argument fails in its entirety.

G. Epic Meets the Pleading Standard for Fraud.

TCS argues that Epic's cause of action for fraud should be dismissed because Epic fails to plead the elements of such a claim with sufficient particularity. Mot. at 35. TCS is wrong.

Rule 9(b) requires that "the circumstances constituting fraud or mistake" must be stated "with particularity." Fed. R. Civ. P. 9(b). "This ordinarily requires describing the 'who, what, when, where, and how' of the fraud, although the exact level of particularity that is required will necessarily differ based on the facts of the case." *AnchorBank, FSB v. Hofer*, 649 F.3d 610, 615 (7th Cir. 2011). Under Rule 9(b), "[m]alice, intent, knowledge, and other condition of mind of a person may be averred generally." *Hefferman v.* Bass, 467 F.3d 596, 601 (7th Cir. 2006) (alteration in original). Furthermore, "Rule 9(b) does not require a plaintiff to demonstrate that a representation was indeed false." *Id.*

1. Epic's Fraud Claim is Pled with Sufficient Particularity.

TCS argues that Epic's fraud allegations are "vague and conclusory references to a conspiracy, fraudulent conduct, stealing, and a 'scheme.'" Mot. at 36. TCS claims that "Epic does not explain how this 'scheme' meets the required elements of a fraud claim in Wisconsin." *Id.* TCS further argues that Epic's allegations do not contain sufficient detail regarding the "who, what, when, where, and how" of the alleged fraud. *Id*.

In the Amended Complaint, Epic alleges that "[w]hen TCS employees registered for access to Epic's system, agreeing to abide by the conditions that govern access to the system, at least one of them claimed to be a Kaiser employee for the purpose of avoiding the UserWeb Access Agreement and gaining customer-level access to the UserWeb." Am. Compl. ¶ 106. Epic further alleges that other "TCS employees repeatedly accessed Epic's computer network, claiming, through the use of fraudulently obtained log-in credentials, to be persons other than themselves, and thus misrepresenting that most basic information to Epic." *Id.* Epic also alleges that, shortly after Epic suspended the TCS employee's account, the TCS employee sent two emails seeking reactivation of his account, on June 24, 2014 and June 30, 2014. *Id.* ¶¶ 43-44. "The first email on June 24 included a signature line indicating that his title was 'QA Lead, Kaiser Permanente.' The second email on June 30 included a different signature line indicating that [the TCS employee] was actually an 'Onshore Test Lead' for TATA Consultancy Service as well a [sic] 'QA Lead' title for Kaiser." *Id.*

Thus, Epic has alleged sufficient detail of TCS's fraud, including the "who" (the TCS employee, with TCS's knowledge), the "what" (the TCS employee representing that he was a

Kaiser employee, using a "kp.org" email address, and altering his email signature line), the "when" (at the time the TCS employee registered, before June 2014), the "where" (in the registration for credentials, and the emails), and the "how" (by falsely identifying himself as a Kaiser employee instead of a consultant to gain access offered to customers) of TCS' fraud. *See, e.g.*, *AnchorBank*, 649 F.3d at 615 (complaint alleging the steps and net result of defendant's collusive trading stated with particularity the scheme to defraud).

The case cited by TCS, *Muwonge v. Eisenberg*, No. 07-C-0733, 2008 WL 753898 (E.D. Wis Mar. 19, 2008), is easily distinguished here. In *Muwonge*, the plaintiff alleged that the defendant had agreed to make the plaintiff a named partner in their firm. *Id.* at *7. The plaintiff alleged that the defendant then engaged in fraud by arbitrarily failing to change the firm name in breach of the agreement and defendants' fiduciary duties. *Id*. The court found that the plaintiff had not pled his claim with sufficient particularity, concluding: "Simply stated, the plaintiff has failed to provide sufficient details regarding the alleged false representation, and has failed to even generally allege that the defendants made the false representation with the intent to defraud." *Id.* at *8.

In contrast, here, Epic has clearly alleged that TCS's employee made the false representations with the intent to defraud. *See, e.g.*, Am. Compl. ¶ 42 ("[The TCS employee] appears to have intentionally misrepresented himself as a Kaiser employee, when he knew his representation was false, for the purpose of . . . gaining customer-level access authorization to Epic's UserWeb"). In addition, as discussed below, Epic's fraud claim is distinct from its breach of contract claim.

2. Epic's Fraud Claim is Not a Breach of Contract Claim.

TCS argues that Epic's claim should be dismissed because "Epic has simply repackaged its breach of contract claim as a fraud claim." Mot. at 36. TCS cites *RxUSA, Inc. v. Capital Returns, Inc.*, No. 06-C-00790, 2007 WL 2712958, *11 (E.D. Wis. Sept. 14, 2007), for the proposition that "[f]ailure to fulfill contractual obligations does not create tort liability." TCS's argument conveniently omits, however, the court's very next sentence in that opinion: "[A] contractual relationship does not cut off tort liability, if the tort claim can be brought independent of contractual obligation." *Id.* In any event, the quoted language referred to the plaintiff's claims for breach of warranty, negligence, and breach of fiduciary duty. *Id.* at *10-11. The court dismissed the breach of fiduciary duty claims on the grounds that the defendants had no duty to the plaintiffs apart from their contractual obligations under a Service Agreement, and consequently the claim arose under contract, not tort law. *Id.*

TCS also cites *Ice Bowl, LLC v. Weigel Broad, Co.*, 14 F. Supp. 2d 1080, 1082 (E.D. Wis. 1998), which considered the narrow (and unrelated) issue of whether the economic loss doctrine should apply to claims for misrepresentation and fraud in the inducement of a contract. Tellingly, TCS does not compare Epic's breach of contract allegations to its fraud allegations in its attempt to show that the two are allegedly the same. In its claim for breach of contract, Epic alleges that:

> Defendants have breached the TCS America Agreement and failed to protect Epic's confidential and proprietary information by, among other things, improperly utilizing UserWeb access credentials through non-registered employees and employees who do not require access to consult for an Epic customer; downloading Epic's confidential and proprietary information – including Program Property, Confidential Information, and Documentation as defined in the TCS America Agreement – and then sending that information to India for purposes other than implementing the Program Property on Epic's or its customer's behalf; and using

> Epic's confidential and proprietary information – including Program Property, Confidential Information, and Documentation – to develop and enhance Defendants' software designed to compete with Epic." Am. Compl. ¶ 94.

By contrast, in its claim for fraud (as discussed above), Epic alleges that a TCS employee, with TCS's knowledge, represented that he was a Kaiser employee, used a "kp.org" email address, and altered his email signature when he registered for UserWeb and in June 2014 emails in order to falsely identify himself as a Kaiser employee instead of a consultant to gain access offered to customers. This conduct is clearly distinct from TCS's breach of the TCS America Agreement, as alleged in the Amended Complaint, and for this reason TCS's argument fails.

H. **Epic's Conversion Claim Is Proper as a Matter of Law.**

TCS contends that, in addition to being preempted by the WUTSA, Epic's conversion claim fails as a matter of law because it is "based entirely on intangible electronic files that Epic alleges TCS downloaded from UserWeb." Mot. at 38. However, TCS admits that "a conversion claim based on intangible rights may be available if there is 'some tangible thing to which the intangible rights attach which is capable of being wrongfully controlled.'" *Id.* TCS argues that "[e]ven if intangible property were subject to conversion, Epic has not alleged any interference with its possession of the allegedly downloaded files." *Id.* Rather than addressing Epic's allegations, TCS invents facts that Epic could have alleged, stating "Epic does not allege, for example, that TCS deleted or altered any files, or otherwise rendered them unavailable to Epic." *Id.*

Unlike the cases cited by TCS, Epic does not allege that TCS converted software or funds. *See Lands' End, Inc. v. Genesys Software Systems, Inc.*, No. 13–cv–38–bbc, 2014 WL 266630, at *3 (W.D. Wis. Jan. 24, 2014) (motion for summary judgment on claim for conversion of software); *Third Educ. Grp., Inc. v. Phelps*, No. 07-c-1094, 2009 WL 2150686, at *7 (E.D.

Wis. May 15, 2009) (motion for summary judgment with respect to conversion of trademark and domain names); *Maryland Stuffing Servs. Inc. v. Manpower, Inc.*, 936 F. Supp. 1494, 1507 (E.D. Wis. 1996) (conversion claim based on theory that the plaintiffs' intangible right to funds was wrongfully converted by the defendant). Rather, Epic alleges that "Defendants willfully took, controlled, interfered with, and/or deprived Epic of *documents and information* without Epic's consent and without lawful authority, including information and documents that do not comprise trade secrets." Am. Compl. ¶ 114 (emphasis added). Notably, TCS does not cite any cases that support the proposition that documents or electronic files are not proper subjects of a conversion claim.

In fact, other jurisdictions have found that electronic documents *are* a proper subject of conversion claims. "Courts dealing with this issue have begun to update the tort of conversion so that it keeps pace with the contemporary realities of widespread computer use." *Aventa Learning, Inc. v. K12, Inc.*, 830 F. Supp. 2d 1083, 1105-06 (W.D. Wash. 2011) (denying motion to dismiss conversion claim where complaint alleged that electronic files were copied, accessed, and destroyed, without authorization); *E.I. DuPont de Nemours and Co. v. Kolon Indus., Inc.*, 688 F. Supp. 2d 443, 455 (E.D. Va. 2009) ("claim for conversion, even if based exclusively on the transfer of copies of electronic information, survives [defendant's] [m]otion to [d]ismiss"); *Thyroff v. Nationwide Mut. Ins. Co.*, 864 N.E.2d 1272, 1278 (N.Y. 2007) ("[T]he tort of conversion must keep pace with the contemporary realities of widespread computer use," and therefore, "electronic records that [are] stored on a computer . . . [are] subject to a claim of conversion . . ."); *Volodarsky v. Moonlight Ambulette Serv.*, Inc., 996 N.Y.S.2d 121, 122 (N.Y. App. Div. 2014) (electronic documents stored on a computer may be the subject of a conversion claim just as printed versions of the documents may).

Accordingly, Epic's claim that TCS has converted its electronic documents and information is proper, and TCS's motion to dismiss should be denied.

CONCLUSION

TCS's motion to dismiss is wholly unfounded. The plausibility argument must be rejected out of hand, as the allegations in the Amended Complaint provide more than sufficient support for the claims brought against TCS, and evidence produced by TCS since the Amended Complaint was filed substantiates those allegations. Further, TCS fails to raise any valid challenges to Epic's individual causes of action. For the foregoing reasons, Epic respectfully requests that the Court deny the motion to dismiss in its entirety.

Dated: March 11, 2015

/s/ Nick G. Saros

Brent Caslin
bcaslin@jenner.com
Nick G. Saros
nsaros@jenner.com
Kate T. Spelman
kspelman@jenner.com
JENNER & BLOCK LLP
633 West 5th Street Suite 2600
Los Angeles, CA 90066
Tel: 213-239-5100
Fax: 213-230-5199

Anthony A. Tomaselli
aat@quarles.com
Kristin G. Noel
kristin.noel@quarles.com
Stacy A. Alexejun
stacy.alexejun@quarles.com
QUARLES & BRADY LLP
33 East Main Street, Suite 900
Madison, WI 53703
Tel.: 608.251.5000
Fax: 608.251.9166

Attorneys for Plaintiff Epic Systems Corporation

CERTIFICATE OF SERVICE

I hereby certify that on March 11, 2015, I caused a true and correct copy of the foregoing Opposition to Defendants' Motion to Dismiss Plaintiffs' Amended Complaint to be served on all counsel of record via the Court's ECF filing system.

/s/ Nick G. Saros
By: Nick G. Saros